AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph [0047] beginning on page 18, as follows:

[0047] TMP3 = Rot2(TMP2) + TMP2 + 1

The instruction code set S127 includes a plurality of instruction codes that indicates to call the rotational module B144 with the variable ~~TMP2~~ TMP3, and to store the result of the operation in a variable TMP4.

TMP4 = Rot4(TMP3) XOR TMP3

The instruction code set S128 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP4 and the data M1, and to store the result in a variable TMP5.

Please amend the paragraph [0050] beginning on page 19, as follows:

[0050] TMP9 = TMP8 + K3

The instruction code set S133 includes a plurality of instruction codes that indicates to call the rotation module A143 with the variable TMP9, and to store the result of the operation in a variable TMP10.

TMP10 = Rot2(TMP9) + TMP9 + 1

The instruction code set S134 includes a plurality of instruction codes that indicates to call the rotation module ~~A143~~ D146 with the variable TMP7 and the variable TMP10, and to store the result of the operation in a variable TMP11.

Please amend the paragraph [0052] beginning on page 20, as follows:

[0052] TMP13 = TMP12 + K4

The instruction code set 137 includes a plurality of instruction codes that indicates to call the rotation module A143 with the variable ~~TMP14~~ TMP13, and to store the result of the operation in a variable TMP14.

TMP14 = Rot2(TMP13) + TMP13 + 1

The instruction code set S138 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP14 and the variable TMP4, and to store the result of the operation in a variable TMP15.

Please amend the paragraph [0054] beginning on page 21, as follows:

[0054] Transmission program 134

The transmission program 134 (not depicted) is composed of a plurality of instruction codes arranged in order, and includes a plurality of instruction codes that indicates to receive the specification of data and the specification of the transmission destination device from the caller program, and to control the communication unit 106 to cause the specified data to be transmitted to the specified transmission destination device.

Please amend the paragraph [0057] beginning on page 22, as follows:

[0057] Hard disk unit 202

The hard disk unit 202 stores the key 222 and is provided with a region for storing encrypted content 221, as shown in FIG. 8. The encrypted content 221 corresponds to the key 222.

The encrypted content 221 and the key 222 are respectively identical to the encrypted content 126 and the key 123 stored on the hard disk 102 of the content server 100.

Please amend the paragraph [0067] beginning on page 25, as follows:

[0067] The instruction code set S217 includes a plurality of instruction codes that indicates to write the single decrypted block generated by the decryption program 234 to the decrypted ~~encrypted~~ content region 236 of the memory 203.

The instruction code set S218 includes a plurality of instruction codes that indicates to pass control to the instruction code set S214.

Please amend the paragraph [0069] beginning on page 26, as follows:

[0069] The instruction code set S218 includes a plurality of instruction codes that indicates to read at least one decrypted block from the decrypted ~~encrypted~~ content region 236 of the memory unit 203.

The instruction code set S219 includes a plurality of instruction codes that indicates to generate the video data and audio data from the read decrypted block, to convert the generated video data and audio data, and to output the resulting video signals and audio signals to the monitor 208 via the display control unit 205.

Please amend the paragraph [0074] beginning on page 28, as follows:

[0074] The instruction code set S223 includes an instruction code which defines data M1 and an instruction code which defines data M2. The data M1 are the 32 most significant bits of the received ciphertext M, and the data M2 are the 32 least significant bits of the received ciphertext M.

The instruction code set S224 includes a plurality of instruction codes that indicates to take the XOR operation ~~sum~~ of the data M1 and the data M2, and to store the result of this operation in a variable TMP1.

Please amend the paragraph [0076] beginning on page 28, as follows:

[0076] The instruction code set S226 includes a plurality of instruction codes that indicates to call the rotational module A244 with the variable TMP2, and to store the result of the operation in a variable TMP3.

TMP3 = Rot2(TMP2) + TMP2 + 1

The instruction code set S227 includes a plurality of instruction codes that indicates to call the rotational module B245 with the variable ~~TMP2~~ TMP3, and to store the result of the operation in a variable TMP4.

Please amend the paragraph [0082] beginning on page 30, as follows:

[0082] The instruction code set S237 includes a plurality of instruction codes that indicates to call the rotation module A244 with the variable ~~TMP14~~ TMP13, and to store the result of the operation in a variable TMP14.

TMP14 = Rot2(TMP13) + TMP13 + 1

The instruction code set S238 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP14 and the variable TMP4, and to store the result of the operation in a variable TMP15.

Please amend the paragraph [0094] beginning on page 35, as follows:

[0094] In order to avoid complicated expressions, let $m_i = p_i - 1$.

First it is calculated that

$u_2 = m_1 \times (m_1^{-1} \bmod (m_2/\mathrm{GCD}(m_1, m_2))) \times (c_2 - c_1) + c_1$

where GCD(a,b,c...) indicates the Greatest Common Divisor of a, b, c ....

Next, it is calculated that

$u_3 = (m_1 \times m_2) \times ((m_1 \times m_2)^{-1} \bmod (m_3/\mathrm{GCD}(m_1, m_2, m_3))) \times (c_3 - u_2) + u_2$, and

$u_4 = (m_1 \times m_2 \times m_3) \times ((m_1 \times m_2 \times m_3)^{-1} \bmod (m_4/\mathrm{GCD}(m_1, m_2, m_3, \underline{m_4}))) \times (c_4 - u_3) + u_3$.

Similarly, $u_1, u_2, \ldots, u_{k-1}$ are calculated in this order. Lastly, the following is calculated:

$u_k = (m_1 \times m_2 \times m_3 \times \ldots \times m_{k-1}) \times ((m_1 \times m_2 \times \ldots \times m_{k-1})^{-1} \bmod (m_k/\mathrm{GCD}(m_1, m_2, m_3, m_4, \ldots, \underline{m_k}))) \times (c_k - u_{k-1}) + u_{k-1}$.

Please amend the paragraph [0119] beginning on page 44, as follows:

[0119] **3.1 Construction of addition module 601**

The addition module 601 is a program that calculates and outputs data a + b for input data a and b, similarly to the addition module 243. As shown in FIG. 18, the addition module 601 is composed of a conversion unit 611, a main calculation unit 612, and an inverse conversion unit 613. The conversion unit 611 includes a parameter storage unit 621 and a scalar multiplication unit 622. The main calculation unit 612 includes a parameter storage unit 623 and an elliptic curve addition unit 624, and the inverse conversion unit 613 includes a parameter storage unit 625, a reduction unit 626, and a discrete logarithm calculation unit 627.

Please amend the paragraph [0139] beginning on page 51, as follows:

[0139] **3.9 Notes**

In the addition module 601, scalar multiplications in the group E(GF(p)) × E(GF(q)) ~~E(GF(p) × GF(q))~~ formed by the elliptic curve over Z/nZ are performed by the conversion unit, and the discrete logarithm problem in the subgroup E(GF(p)) is solved by the inverse conversion unit.

In the case where a person attempting to analyze the program discovers that that a power calculation is being performed in the in the conversion unit but does not know p and q, only the

inverse conversion unit is difficult to analyze.

Please amend the paragraph [0140] beginning on page 51, as follows:

[0140] However, if n is large enough to make the prime factorization difficult (of the order of 1024 bits, for instance), it is difficult to obtain p and q since to do so would require a prime factorization of n. Without obtaining p and q, it is difficult to solve the discrete logarithm problem in the group E(GF(p)) × E(GF(q)) ~~E(GF(p) × GF(q))~~ formed by the elliptic curve over Z/nZ.